

**NET.4.1.A16 Sicherung von Endgeräten in frei zugänglichen Räumen (S)**

Der Funktionsumfang der Endgeräte, die in frei zugänglichen Räumen aufgestellt werden sollen, SOLLTE eingeschränkt werden. Ist dies nicht möglich, SOLLTE das Endgerät in geeigneter Weise vor unbefugtem Zugriff geschützt werden.

**NET.4.1.A17 Wartung von TK-Anlagen (S)**

Die Geräte zur Wartung und Konfiguration der TK-Anlage SOLLTEN mit Passwörtern bzw. PINs abgesichert sein.

### 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

**NET.4.1.A18 Erhöhter Zugangsschutz (H)**

Die TK-Anlage SOLLTE in einem separaten sowie geeignet gesicherten Raum untergebracht sein. Der Zutritt und Zugang zur TK-Anlage SOLLTE nur einem eingeschränkten Personenkreis möglich sein. Externe SOLLTEN nur beaufsichtigt Zugang zur Anlage erhalten.

**NET.4.1.A19 Redundanter Anschluss (H)**

Der Anschluss der TK-Anlage SOLLTE redundant ausgelegt sein. Bei IP-basierten TK-Anlagen SOLLTE ein zusätzlicher PSTN-Anschluss vorhanden sein.

## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ veröffentlicht.





## NET.4.2 VoIP

### 1. Beschreibung

#### 1.1. Einleitung

Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Um Signalisierungsinformationen zu übertragen, beispielsweise bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten wie Sprache oder Video werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils benötigt, um eine Multimediaserverbindung aufzubauen und aufrechtzuerhalten. Bei einigen Verfahren wird nur ein Protokoll sowohl für die Signalisierung als auch für den Medientransport benötigt.

#### 1.2. Zielsetzung

Dieser Baustein betrachtet die Sicherheitsaspekte der Endgeräte und Vermittlungseinheiten (Middleware) von VoIP. Die hier beschriebenen Komponenten gleichen hinsichtlich ihrer Funktionalität den im Baustein NET 4.1 *TK-Anlagen* beschriebenen Telekommunikationsanlagen.

#### 1.3. Abgrenzung und Modellierung

Der Baustein NET.4.2 *VoIP* ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP eingesetzt wird. Da VoIP über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* oder NET.3.2 *Firewall* geeignet mit zu berücksichtigen.

In diesem Baustein werden die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP betrachtet. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein Datennetz aus, ist dieser Baustein ebenfalls anzuwenden.

Die spezifischen Gefährdungen und Anforderungen von klassischen TK-Anlagen sowie Hybrid-Anlagen werden in dem Baustein NET 4.1 *TK-Anlagen* betrachtet.

Oft wird VoIP-Software nicht auf eigens dafür vorgesehene Hardware betrieben, sondern auf Standard-IT. Werden Softphones auf Clients installiert, sollten die Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* sowie der betriebssystemspezifischen Bausteine berücksichtigt werden. Wird Software für VoIP auf Servern betrieben, sollten neben den Anforderungen der betriebssystemspezifischen Bausteine die Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* erfüllt werden.

VoIP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.1.5 *Protokollierung*, sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.2 *VoIP* von besonderer Bedeutung.

#### 2.1. Fehlerhafte Konfiguration der VoIP-Middleware

Eine VoIP-basierte Telefonanlage kann in ähnlicher Weise von Fehlkonfigurationen betroffen sein wie eine leitungsvermittelnde Telefonlösung. So könnten beispielsweise Telefonbenutzenden falsche Telefonnummern zugeordnet

werden oder die gesamte Telefoninfrastruktur könnte ausfallen. Auch tendenziell unkritische Fehler, wie ein falsch geschriebener Name im Telefonbuch, können nicht ausgeschlossen werden.

Wird mittels VoIP kommuniziert, sind in der Regel mehrere IT-Systeme beteiligt. Wird SIP als Initialisierungsprotokoll eingesetzt, werden meist Systeme wie *Registrare*, *SIP-Proxy-Server* und *Location-Server* für die Kommunikation benötigt. Ändert sich die VoIP-Infrastruktur, müssen alle IT-Systeme angepasst werden. Dadurch können leicht Konfigurationsfehler entstehen. Auch wenn sich alle Dienste auf einem Server befinden, müssen diese häufig einzeln konfiguriert werden. Wird nur ein System fehlerhaft geändert, kann die gesamte Telefoninfrastruktur möglicherweise nicht mehr genutzt werden.

## 2.2. Fehlerhafte Konfiguration der VoIP-Komponenten

Unabhängig davon, ob es sich bei VoIP-Komponenten um dedizierte Hardware („Appliances“) oder softwarebasierte Systeme handelt, ist die Konfiguration entscheidend für die fehlerfreie Funktion des Systems. Neben den Einstellungen zur Signalisierung, die bei der Planung festgelegt wurden, spielt das Übertragungsverfahren für die Medienströme eine wichtige Rolle. Durch ein Kompressionsverfahren kann die Größe der Datenpakete mit den Sprachinformationen verkleinert werden.

Durch die fehlerhafte Konfiguration des Übertragungsverfahrens können Probleme bei der Übertragung auftreten. Wird ein ungeeignetes Verfahren eingesetzt und werden Sprachinformationen zu stark komprimiert, verschlechtert sich oft die Sprachqualität. Wird hingegen ein Verfahren gewählt, das eine zu geringe Kompression vornimmt, wird der Nachrichtenstrom nicht ausreichend vermindert und das Datennetz kann überlastet werden.

## 2.3. Abhören von Telefongesprächen

Wenn Telefongespräche oder Daten unverschlüsselt übertragen werden, könnten Angreifende grundsätzlich Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmern vermittelnden TK-Anlage lauschen. Bei VoIP können Telefongespräche und Datenübertragungen sogar einfacher als bei klassischen TK-Anlagen abgehört werden. Alle Sprachinformationen werden innerhalb eines Medienstroms, beispielsweise mit dem Realtime Transport Protocol (RTP), übertragen. Durch Techniken wie Spoofing und Sniffing stehen bei VoIP den Angreifenden auch alle Möglichkeiten von Angriffen in Datennetzen zur Verfügung.

Bei vielen TK-Anlagen können Anrufende den Empfangenden Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, versenden diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von einem Angreifenden abgefangen und angehört werden.

## 2.4. Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinen Benutzenden persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besuchende frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystmen. Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

Beim Einsatz von VoIP-Telefonen in frei zugänglichen Bereichen können weitere Aspekte relevant sein. Denn sie haben einen hohen Software-Anteil und werden häufig in Datennetzen betrieben, die auch für andere IT-Anwendungen genutzt werden. Angreifende könnten deshalb durch den direkten Zugriff auf Geräteinformationen versuchen, Schwachstellen in der VoIP-Software auszunutzen oder selbst schädliche Software zu installieren.

VoIP-Telefone müssen an ein Datennetz angeschlossen sein. Angreifende könnten an diesen Netzanschluss ein mobiles IT-System anschließen und so unter Umständen auf das von außen durch eine Firewall geschützte interne Netz zugreifen. Diesen Zugang können sie möglicherweise für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit ausnutzen.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.2 VoIP aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singularen oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### NET.4.2.A1 Planung des VoIP-Einsatzes (B)

Die Bedingungen, unter denen VoIP eingesetzt werden soll, MÜSSEN festgelegt werden. Es MUSS unter anderem entschieden werden, ob vollständig oder partiell auf VoIP umgestiegen werden soll. Besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen SOLLTEN vorab ermittelt werden. Geeignete Signalisierungs- und Medientransportprotokolle MÜSSEN vor dem Einsatz ausgewählt werden.

Es SOLLTE entschieden werden, ob und wie die VoIP-Infrastruktur an öffentliche (Daten-)Netze angebunden werden soll. Die Kapazitäten und das Design von vorhandenen Datennetzen SOLLTEN bei der Planung berücksichtigt werden.

#### NET.4.2.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

#### NET.4.2.A3 Sichere Administration und Konfiguration von VoIP-Endgeräten (B)

Nicht benötigte Funktionen der Endgeräte MÜSSEN deaktiviert werden. Die Konfigurationseinstellungen DÜRFEN NICHT unberechtigt geändert werden. Alle Sicherheitsfunktionen der Endgeräte SOLLTEN vor dem produktiven Einsatz getestet werden. Die eingesetzten Sicherheitsmechanismen und die verwendeten Parameter SOLLTEN dokumentiert werden.

#### NET.4.2.A4 Einschränkung der Erreichbarkeit über VoIP (B)

Es MUSS entschieden werden, wie externe Gesprächspartner und -partnerinnen auf die VoIP-Architektur zugreifen können. Es MUSS verhindert werden, dass IT-Systeme aus unsicheren Netzen direkte Datenverbindungen auf die VoIP-Komponenten der Institution aufbauen können. Wenn alle ein- und ausgehenden Verbindungen über ein zentrales IT-System abgewickelt werden sollen, SOLLTE sichergestellt werden, dass alle Signalisierungs- und Sprachinformationen zwischen dem öffentlichen und dem privaten Datennetz nur über dieses autorisierte IT-System ausgetauscht werden.

#### NET.4.2.A5 Sichere Konfiguration der VoIP-Middleware (B)

Die VoIP-Komponenten MÜSSEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Die Default-Konfigurationen der VoIP-Middleware MÜSSEN vor der produktiven Inbetriebnahme angepasst werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch sachkundige Dritte anhand der Dokumentation nachvollzogen und wiederholt werden können. Alle nicht benötigten Dienste der VoIP-Middleware MÜSSEN deaktiviert werden.

#### NET.4.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

#### NET.4.2.A7 Erstellung einer Sicherheitsrichtlinie für VoIP (S)

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweiten Sicherheitsrichtlinie aufgenommen werden. In dieser Sicherheitsrichtlinie SOLLTEN alle allgemeinen sicherheitstechnischen Vorgaben konkretisiert werden. Außerdem SOLLTEN in der Richtlinie die Vorgaben für den Betrieb und die Nutzung der VoIP-Komponenten geregelt sein. Hierbei SOLLTEN auch die verschiedenen VoIP-Funktionen, wie zum Beispiel Voicemails, betrachtet werden. Die VoIP-Sicherheitsrichtlinie SOLLTE allen beteiligten Personen und Gruppen zugänglich und bekannt sein.

#### NET.4.2.A8 Verschlüsselung von VoIP (S)

Es SOLLTE entschieden werden, ob und welche Sprach- und Signalisierungsinformationen verschlüsselt werden sollen. Generell SOLLTEN alle VoIP-Datenpakete, die das gesicherte LAN verlassen, durch geeignete Sicherheitsmechanismen geschützt werden. Die Benutzenden SOLLTEN über die Nutzung der VoIP-Verschlüsselung informiert werden.

#### NET.4.2.A9 Geeignete Auswahl von VoIP-Komponenten (S)

Bevor VoIP-Komponenten beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste SOLLTEN die am Markt erhältlichen Produkte bewertet werden. Diese Anforderungsliste SOLLTE alle Merkmale zur Erreichung des angestrebten Sicherheitsniveaus umfassen. Es SOLLTE geregelt werden, wie die am Markt erhältlichen Produkte gemäß der Anforderungsliste bewertet werden können.

#### NET.4.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

#### NET.4.2.A11 Sicherer Umgang mit VoIP-Endgeräten (S) [Benutzende]

Benutzende, die VoIP-Endgeräte einsetzen, SOLLTEN über die grundlegenden VoIP-Gefährdungen und Sicherheitsmaßnahmen informiert sein. Außerdem SOLLTEN sie geeignete Passwörter zur Absicherung von Voicemails auswählen.

#### NET.4.2.A12 Sichere Außerbetriebnahme von VoIP-Komponenten (S)

Wenn VoIP-Komponenten außer Betrieb genommen oder ersetzt werden, SOLLTEN alle sicherheitsrelevanten Informationen von den Geräten gelöscht werden. Nach dem Löschgong SOLLTE überprüft werden, ob die Daten auch tatsächlich erfolgreich entfernt wurden. Vertrauliche Informationen SOLLTEN auch von Backup-Medien gelöscht werden. Alle Beschriftungen, insbesondere der Endgeräte, SOLLTEN vor der Entsorgung entfernt werden. Es SOLLTE frühzeitig mit Herstellenden, Vertreibenden beziehungsweise Service-Unternehmen geklärt werden, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind.

#### NET.4.2.A13 Anforderungen an eine Firewall für den Einsatz von VoIP (S)

Es SOLLTE überprüft werden, ob die bestehende Firewall für den Einsatz von VoIP angepasst werden kann. Ist dies nicht der Fall, SOLLTE eine zusätzliche Firewall hierfür beschafft und installiert werden.

### 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

**NET.4.2.A14 Verschlüsselung der Signalisierung (H)**

Die Integrität und Vertraulichkeit der Signalisierungsinformationen SOLLTE durch geeignete kryptografische Verfahren gewährleistet werden. Nicht nur die Nutzdaten, sondern auch die Authentisierungsdaten SOLLTEN durchgängig verschlüsselt werden. Der Zugriff auf das VoIP-Gateway SOLLTE durch VoIP-Adressen und H.323-Identitäten so weit wie möglich eingeschränkt werden. Es SOLLTEN zusätzlich Ende-zu-Ende-Sicherheitsmechanismen für den Medientransport und die Signalisierung benutzt werden. Es SOLLTE dokumentiert werden, wie die Signalisierung geschützt wird.

**NET.4.2.A15 Sicherer Medientransport mit SRTP (H)**

Mediendaten und Informationen zur Steuerung dieser Daten, die über das Real-Time Transport Protocol (RTP) übertragen werden, SOLLTEN in geeigneter Weise geschützt werden. Die Nutzdaten SOLLTEN durch den Einsatz von Secure Real-Time Transport Protocol (SRTP) beziehungsweise Secure Real-Time Control Protocol (SRTCP) geschützt werden. Die sicherheitsrelevanten Optionen der Implementierung des Protokolls SOLLTEN dokumentiert werden.

**NET.4.2.A16 Trennung des Daten- und VoIP-Netzes (H)**

Das VoIP-Netz SOLLTE in geeigneter Weise vom Datennetz getrennt werden. Es SOLLTE geregelt werden, wie mit Geräten umzugehen ist, die auf das VoIP- und Datennetz zugreifen müssen. VoIP-Endgeräte in einem VoIP-Netz SOLLTEN nur die vorgesehenen VoIP-Verbindungen zu anderen IT-Systemen aufbauen können.

## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ veröffentlicht.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-5 zu „Security Considerations for Voice Over IP Systems“ veröffentlicht.





## NET.4.3 Faxgeräte und Faxserver

### 1. Beschreibung

#### 1.1. Einleitung

In diesem Baustein werden die Sicherheitsaspekte der Informationsübermittlung über marktübliche Faxgeräte sowie Faxserver betrachtet. Die übermittelten Informationen werden als Fax (Kurzform von Telefax) oder seltener auch als Telefaksimile oder Fernkopie bezeichnet. Bei einem herkömmlichen Faxgerät werden von einer Vorlage die darauf aufgezeichneten Inhalte vom Sendegerät Punkt für Punkt abgetastet und zu den Empfangsgeräten übertragen. Das Empfangsgerät baut diese Inhalte wieder Punkt für Punkt auf und gibt sie in der Regel direkt auf Papier aus.

Ein Faxserver hingegen ist ein Dienst, der auf einem Server installiert wird und so anderen IT-Systemen in einem Datennetz ermöglicht, Faxe zu versenden und zu empfangen. Faxserver werden häufig in bereits bestehende E-Mail- oder Groupware-Systeme integriert. So ist es möglich, dass eingehende Fax-Dokumente durch den Faxserver per E-Mail an die Benutzenden zugestellt werden. Abzusendende Dokumente werden entweder über eine Druckerwarteschlange oder per E-Mail an den Faxserver übergeben. In der Regel wird das Dokument zwischen Faxserver und den Clients im Datennetz als Bild-Datei gesendet oder empfangen. Die übermittelte Bild-Datei kann nicht unmittelbar in Textverarbeitungssystemen weiterverarbeitet werden. Hierzu ist in der Regel zunächst eine Texterkennung (OCR, Optical Character Recognition) erforderlich. Von einem Faxserver empfangene und verarbeitete Dokumente lassen sich für gewöhnlich einfach archivieren, beispielsweise durch den Faxserver-Dienst selber, durch Dokumentenmanagementsysteme oder durch die Groupware, die direkt an den Faxserver-Dienst angebunden sind.

#### 1.2. Zielsetzung

Ein Ziel dieses Bausteins ist der Schutz der Informationen, die mithilfe von Faxsendungen übermittelt und verarbeitet werden. Ein weiteres Ziel ist der Schutz der Faxgeräte und Faxserver vor Manipulationen durch Unbefugte. Das Übertragungsmedium spielt bei der Anwendung des Bausteins keine Rolle, sodass die Anforderungen des Bausteins auch für Fax over IP (FoIP) umgesetzt werden sollten.

#### 1.3. Abgrenzung und Modellierung

Der Baustein NET.4.3 *Faxgeräte und Faxserver* ist für jedes Faxgerät und jeden Faxserver im Informationsverbund anzuwenden.

In diesem Baustein werden als technische Basis des Faxversandes marktübliche Stand-Alone-Faxgeräte und Faxserver betrachtet. Zusätzliche Aspekte zu Faxgeräten, die in einem Multifunktionsgerät (All-in-one-Gerät) zu finden sind, werden gesondert in dem Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* behandelt. Zum Schutz der Informationen, die auf Faxservern verarbeitet, angeboten, gespeichert und darüber übertragen werden, sollten der Baustein SYS.1.1 *Allgemeiner Server* sowie die jeweiligen betriebssystemspezifischen Bausteine betrachtet werden. Informationen zur richtigen Archivierung können dem Baustein OPS.1.2.2 *Archivierung* entnommen werden.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.3 *Faxgeräte und Faxserver* von besonderer Bedeutung.

## 2.1. Unzureichende oder falsche Versorgung mit Verbrauchsgütern

Faxgeräte empfangen Dokumente und drucken diese in der Regel direkt auf Papier aus. Für einen reibungslosen und unterbrechungsfreien Betrieb eines Faxgerätes müssen Verbrauchsgüter wie Papier und Toner in ausreichender Menge vorhanden sein. Ist dies nicht gegeben, können oft keine Fax-Dokumente empfangen werden. Außerdem können keine Sendebestätigungen ausgedruckt werden, die eventuell zwingend benötigt werden.

## 2.2. Fehlerhafte Faxübertragung

Auf dem Übertragungsweg zwischen Sendegerät und Empfangsgerät eines Fax-Dokuments können zahlreiche Störungen auftreten. Dies kann dazu führen, dass die zu übermittelnden Fax-Dokumente unvollständig oder unlesbar sind oder gar nicht bei den Empfangenden ankommen. Entscheidungen, die von diesen Informationen abhängig sind, können fehlerhaft sein und somit hohe Schäden verursachen.

Zeitverzögerungen, die entstehen, weil die Probleme erst erkannt werden müssen und das Dokument neu gesendet werden muss, können zu weiteren Komplikationen führen. Oft haben die Sendenden oder Empfangenden gar keine Möglichkeiten, den Übertragungsweg zu beeinflussen, sodass sie warten müssen, bis die Störung durch Dritte behoben wurde. Häufig glauben die Absendenden sogar, dass das Fax-Dokument ordnungsgemäß an die gewünschten Adressaten übermittelt wurden und die hierdurch entstehenden Probleme werden erst sehr spät erkannt.

Zusätzlich kann nicht ausgeschlossen werden, dass ein Fax-Dokument an das falsche Empfangsgerät übermittelt wurde, beispielsweise weil eine Fehlschaltung im öffentlichen Telekommunikationsnetz vorliegt. Ebenso ist denkbar, dass bei Faxgeräten Rufnummern falsch gewählt oder Zielwahltasten falsch programmiert werden. Wird ein Faxserver verwendet, können die Rufnummern ebenfalls falsch eingegeben oder falsch im Adressbuch abgespeichert werden. Dadurch können unter Umständen vertrauliche Informationen an unbefugte Personen übermittelt werden.

## 2.3. Manipulation von Adressbüchern und Verteilerlisten

In Faxgeräten können häufig Adressbücher und Verteilerlisten geführt werden. Wird ein Faxserver genutzt, können in der Regel über die Groupware ähnliche Adressbücher und Verteilerlisten an einer zentralen Stelle geführt werden, die von mehreren Benutzenden verwendet werden können. In den Adressbüchern können Nummern von Empfangenden gespeichert werden, sodass diese nicht bei jedem Faxversand neu eingegeben werden müssen. Zudem ist es möglich, über Verteilerlisten eine Gruppe von Empfangenden anzulegen und so Faxsendungen an mehrere Personen gleichzeitig zu verschicken.

Häufig werden einmal programmierte Nummern von Empfangenden oder Verteilerlisten nicht mehr kontrolliert, wenn ein Fax-Dokument versendet werden soll. Wenn Unbefugte die Adressbücher oder die Verteilerlisten am Faxgerät oder in der Groupware ändern, können so vertrauliche Informationen an die falschen Empfangenden gelangen. Außerdem kann es passieren, dass die vorgesehenen Empfangenden dringend benötigte Informationen nicht erhalten. Beispielsweise könnte eine Faxnummer im Adressbuch ausgetauscht oder weitere Empfängende in die Verteilerliste aufgenommen werden, ohne dass dies von den Verantwortlichen in der jeweiligen Institution bemerkt wird.

## 2.4. Unbefugtes Lesen von Faxsendungen

In fast allen Fällen ist es am wirtschaftlichsten, wenn sich mehrere Benutzende ein Faxgerät teilen. Daher werden diese in der Regel in Räumen aufgestellt, die alle Mitarbeitenden einer Institution betreten können, wie beispielsweise in Druckerräumen. Da hierdurch die Faxgeräte für alle Mitarbeitenden frei zugänglich sind, können auch alle Mitarbeitenden die empfangenen Faxsendungen lesen und so an vertrauliche Informationen gelangen.

## 2.5. Auswertung von Restinformationen in Faxgeräten und Faxservern

Abhängig vom technischen Verfahren, mit dem Faxgeräte Informationen speichern, weiterverarbeiten oder drucken, können nach dem Faxversand und -empfang Restinformationen unterschiedlichen Umfangs im Faxgerät verbleiben. Unbefugte, die in den Besitz des Gerätes oder der entsprechenden Bauteile kommen, können diese Informationen unter Umständen wiederherstellen.

Auf der Festplatte eines Faxservers werden Faxsendungen mindestens so lange gespeichert, bis sie an das Ziel zugestellt werden können. Weiterhin arbeiten moderne Betriebssysteme mit Auslagerungsdateien, die auch Restinformationen enthalten können. Diese Informationen könnten beim Zugriff auf diesen Faxserver unerlaubt ausgewertet werden.

## 2.6. Vortäuschen eines falschen Absendenden bei Faxsendungen

Faxsendungen sind ein beliebtes Medium, um Dokumente, die nur mit einer Unterschrift gültig sind, zu übertragen. Doch auf die gleiche Weise, wie mit einem falschen Namen und einem falschen Briefkopf falsche Absendende vorgetäuscht werden kann, kann auch eine Faxsendung manipuliert werden. So können beispielsweise Unterschriften von anderen Schriftstücken eingescannt und auf das Fax-Dokument kopiert werden. Ein Unterschied, ob es sich um eine tatsächlich getätigte Unterschrift oder um eine reproduzierte Grafikdatei handelt, ist generell nicht zu erkennen. Schäden entstehen dann, wenn Empfangende die darin enthaltenen Informationen als authentisch oder sogar als rechtsverbindlich ansehen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET:4.3 *Faxgeräte und Faxserver* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	Benutzende, Beschaffungsstelle, IT-Betrieb, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### NET.4.3.A1 Geeignete Aufstellung eines Faxgerätes (B) [Haustechnik]

Faxgeräte MÜSSEN so aufgestellt werden, dass eingegangene Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Der Aufstellungsort SOLLTE zudem danach ausgewählt werden, dass ausreichend dimensionierte Telekommunikationsleitungen bzw. -kanäle vorhanden sind. Der Aufstellungsort MUSS über einen geeigneten Netzanschluss für das Faxgerät verfügen. Faxgeräte DÜRFEN NICHT an nicht dafür vorgesehene Netzanschlüsse angeschlossen werden.

#### NET.4.3.A2 Informationen für Mitarbeitende über die Faxnutzung (B)

Alle Mitarbeitenden MÜSSEN auf die Besonderheiten der Informationsübermittlung per Fax hingewiesen werden. Sie MÜSSEN auch darüber informiert sein, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Eine verständliche Bedienungsanleitung MUSS am Faxgerät ausliegen. Die Benutzenden SOLLTEN mindestens eine Kurzanleitung zur eingesetzten Faxclient-Software des Faxservers erhalten. Außerdem MUSS eine Anweisung zur korrekten Faxnutzung ausliegen.

#### NET.4.3.A3 Sicherer Betrieb eines Faxservers (B) [IT-Betrieb]

Bevor ein Faxserver in Betrieb genommen wird, SOLLTE eine Testphase erfolgen. Konfigurationsparameter sowie alle Änderungen an der Konfiguration eines Faxservers SOLLTEN dokumentiert werden. Die Archivierung und Löschung von Faxdaten SOLLTEN geregelt sein. Außerdem MUSS regelmäßig die Verbindung vom Faxserver zur

TK-Anlage beziehungsweise zum öffentlichen Telefonnetz auf ihre Funktion geprüft werden. Es MUSS außerdem sichergestellt werden, dass der Faxserver ausschließlich Fax-Dienste anbietet und nicht für weitere Dienste genutzt wird. Alle nicht benötigten Leistungsmerkmale und Zugänge der eingesetzten Kommunikationsschnittstellen MÜSSEN deaktiviert werden.

### 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

#### NET.4.3.A4 Erstellung einer Sicherheitsrichtlinie für die Faxnutzung (S)

Vor der Freigabe eines Gerätes SOLLTE eine Sicherheitsrichtlinie für die Faxnutzung erstellt werden. Dort SOLLTE die Einsatzart festgelegt sein. Außerdem SOLLTE geregelt werden, wie mit Faxeingängen und -ausgängen umzugehen ist. Zudem SOLLTE eine Regelung zur Behandlung von nicht zustellbaren Faxsendungen erstellt werden. Außerdem SOLLTE die Richtlinie Informationen und Anweisungen zur Notfallvorsorge und Ausfallsicherheit des Faxbetriebes enthalten.

#### NET.4.3.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

#### NET.4.3.A6 Beschaffung geeigneter Faxgeräte und Faxserver (S) [Beschaffungsstelle]

Bevor Faxgeräte oder Faxserver beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand dieser Liste SOLLTEN die infrage kommenden Systeme oder Komponenten bewertet werden. Die Anforderungsliste für Faxgeräte SOLLTE auch sicherheitsrelevante Aspekte umfassen, wie den Austausch einer Teilnehmererkennung, die Ausgabe von Sendeberichten sowie eine Fehlerprotokollierung und Journalführung. Zudem SOLLTEN angemessene zusätzliche Sicherheitsfunktionen anhand des Schutzbedarfs berücksichtigt werden.

Bei einem Faxserver SOLLTEN alle Anforderungen an das IT-System einschließlich Betriebssystem, Kommunikationskomponenten und Applikationssoftware erhoben und berücksichtigt werden. Die Möglichkeit, dass ein Faxserver in ein bestehendes Datennetz und in ein Groupware-System integriert werden kann, SOLLTE bei Bedarf berücksichtigt werden.

#### NET.4.3.A7 Geeignete Kennzeichnung ausgehender Faxsendungen (S) [Benutzende]

Quelle und Ziel jeder Faxsendung SOLLTEN auf allen ausgehenden Faxsendungen ersichtlich sein. Wenn diese Informationen nicht aus dem versendeten Dokument ermittelt werden können, SOLLTE ein standardisiertes Faxdeckblatt benutzt werden. Generell SOLLTE das Faxdeckblatt mindestens den Namen der Institution des Absendenden, den Namen des Ansprechpartners bzw. der Ansprechpartnerin, das Datum, die Seitenanzahl sowie einen Dringlichkeitsvermerk auflisten. Außerdem SOLLTE es die Namen und die Institution der Empfangenden enthalten. Wenn notwendig, SOLLTE das Faxdeckblatt für jedes ausgehende Fax angepasst werden.

#### NET.4.3.A8 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen (S)

Alle Fax-Verbrauchsgüter, aus denen Informationen über die versendeten und empfangenen Fax-Dokumente gewonnen werden können, SOLLTEN vor der Entsorgung unkenntlich gemacht werden oder durch eine zuverlässige Fachfirma entsorgt werden. Die gleiche Vorgehensweise SOLLTE auch bei ausgetauschten informationstragenden Ersatzteilen erfolgen. Wartungsfirmen, die Faxgeräte überprüfen oder reparieren, SOLLTEN zu einer entsprechenden Handhabung verpflichtet werden. Es SOLLTE regelmäßig kontrolliert werden, ob diese Handhabung eingehalten wird.

#### NET.4.3.A9 Nutzung von Sende- und Empfangsprotokollen (S)

Die Übertragungsvorgänge ein- und ausgehender Faxsendungen SOLLTEN protokolliert werden. Dazu SOLLTEN die Kommunikationsjournale marktüblicher Faxgeräte genutzt werden. Verfügen die Faxgeräte über Protokollierungsfunktionen, SOLLTEN diese aktiviert werden. Bei einem Faxserver SOLLTE die Protokollierung ebenso aktiviert werden. Auch SOLLTE entschieden werden, welche Informationen protokolliert werden sollen.

Die Kommunikationsjournale der Faxgeräte und die Protokollierungsdateien SOLLTEN regelmäßig ausgewertet und archiviert werden. Sie SOLLTEN stichprobenartig auf Unregelmäßigkeiten geprüft werden. Unbefugte SOLLTEN nicht auf die Kommunikationsjournale sowie die protokollierten Informationen zugreifen können.

#### **NET.4.3.A10 Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten (S)**

Programmierbare Kurzwahlstellen oder gespeicherte Zieladressen SOLLTEN regelmäßig daraufhin überprüft werden, ob die gewünschte Faxnummer mit der einprogrammierten Nummer übereinstimmt. Nicht mehr benötigte Faxnummern SOLLTEN gelöscht werden. Es SOLLTE in geeigneter Weise dokumentiert werden, wenn ein neuer Eintrag aufgenommen oder eine Zielnummer geändert wird.

### **3.3. Anforderungen bei erhöhtem Schutzbedarf**

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

#### **NET.4.3.A11 Schutz vor Überlastung des Faxgerätes (H) [IT-Betrieb]**

Es SOLLTEN ausreichend Kommunikationsleitungen bzw. -kanäle verfügbar sein. Bei einem Faxserver SOLLTE das voraussichtliche Faxvolumen abgeschätzt werden. Es SOLLTEN entsprechend leistungsfähige Komponenten ausgewählt werden. Die Protokolle von Faxservern SOLLTEN regelmäßig kontrolliert werden, um Engpässen durch Überlastungen rechtzeitig entgegenzuwirken. Nicht mehr benötigte Faxdaten SOLLTEN zeitnah vom Faxserver gelöscht werden.

#### **NET.4.3.A12 Sperren bestimmter Quell- und Ziel-Faxnummern (H)**

Unerwünschte Faxadressen, SOLLTEN blockiert werden. Alternativ SOLLTEN nur bestimmte Rufnummern zugelassen werden. Es SOLLTE geprüft werden, welcher Ansatz in welcher Situation geeignet ist.

#### **NET.4.3.A13 Festlegung berechtigter Faxbedienenden (H) [Benutzende]**

Es SOLLTEN nur wenige Mitarbeitende ausgewählt werden, die auf das Faxgerät zugreifen dürfen. Diese Mitarbeitenden SOLLTEN an kommende Faxsendungen an die Empfangenden verteilen. Den Mitarbeitenden SOLLTE vermittelt werden, wie sie mit dem Gerät umgehen und wie sie die erforderlichen Sicherheitsmaßnahmen umsetzen können. Jeder berechtigte Benutzende SOLLTE darüber unterrichtet werden, wer das Faxgerät bedienen darf und wer für das Gerät zuständig ist.

#### **NET.4.3.A14 Fertigung von Kopien eingehender Faxsendungen (H) [Benutzende]**

Auf Thermopapier gedruckte Faxsendungen, die länger benötigt werden, SOLLTEN auf Normalpapier kopiert oder eingescannt werden. Es SOLLTE berücksichtigt werden, dass auf Thermopapier die Farbe schneller verblasst und somit unkenntlich wird. Die Kopien oder eingescannten Faxsendungen SOLLTEN in geeigneter Weise archiviert werden.

#### **NET.4.3.A15 Ankündigung und Rückversicherung im Umgang mit Faxsendungen (H) [Benutzende]**

Wichtige Faxsendungen SOLLTEN den Empfangenden angekündigt werden, bevor sie versendet werden. Dazu SOLLTE festgelegt werden, welche Dokumente vorab angemeldet werden sollen. Mitarbeitende, die vertrauliche Fax-Dokumente versenden möchten, SOLLTEN angewiesen werden, sich den vollständigen Erhalt von den Empfangenden bestätigen zu lassen. Bei wichtigen oder ungewöhnlichen Faxsendungen SOLLTEN sich wiederum Empfänger von den Absendenden bestätigen lassen, dass das Fax-Dokument von ihnen stammt und nicht gefälscht wurde. Es SOLLTE eine geeignete Kommunikationsform ausgewählt werden, mit dem die Fax-Dokumente angekündigt oder bestätigt werden, beispielsweise per Telefon.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Für den Baustein NET:4.3 Faxgeräte und Faxserver sind keine weiterführenden Informationen vorhanden.



# **INF: Infrastruktur**





## INF.1 Allgemeines Gebäude

### 1. Beschreibung

#### 1.1. Einleitung

Ein Gebäude umschließt alle stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik. Es gewährleistet somit einen Schutz vor äußerer Einflüssen. Daher ist nicht nur das Bauwerk an sich zu betrachten, also Wände, Decken, Böden, Dach, Fenster sowie Türen, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung.

Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von institutionsfremden Personen, wie Besuch, Kundschaft oder Liefernden, betreten wird. Wenn ein Gebäude von verschiedenen Parteien genutzt wird, dann müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die dort tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten. Die im Gebäude installierte Technik soll zudem sicher und effizient betrieben werden können.

#### 1.2. Zielsetzung

In diesem Baustein wird beschrieben, welche Anforderungen zu erfüllen sind, um ein Gebäude aus Sicht der Informationssicherheit optimal zu schützen. Die sich aus den Anforderungen ergebenden Maßnahmen hängen von der Art und Größe der Institution sowie Art und Größe des Gebäudes ab. Anforderungen aus diesem Baustein können auch auf große Liegenschaften mit mehreren Gebäuden oder auf die Nutzung einzelner Gebäudeteile in Mehrparteihäusern übertragen werden.

#### 1.3. Abgrenzung und Modellierung

Der Baustein INF.1 *Allgemeines Gebäude* ist für jedes Gebäude einmal anzuwenden.

Dieser Baustein betrachtet technische und nicht-technische Sicherheitsaspekte bei der Planung und Nutzung von typischen Gebäuden für Unternehmen und Behörden. Dabei wird der gesamte Lebenszyklus von Gebäuden aus Sicht der Informationssicherheit betrachtet, beginnend von der Erstellung eines Anforderungskataloges, über die Konzeption, Einrichtung, Nutzung bis hin zu Umbauten oder dem Auszug.

Die Verkabelung in einem Gebäude wird in dem Baustein INF.12 *Verkabelung* gesondert betrachtet, spezielle Räumlichkeiten, wie Serverräume oder Archivräume, in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Der Umgang mit Fremdpersonal ist im Baustein ORP.1 *Organisation* geregelt.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.1 *Allgemeines Gebäude* von besonderer Bedeutung.

### 2.1. Feuer

Gebäude und Einrichtung können durch ein Feuer schwer beschädigt, Menschen schwer verletzt oder getötet werden. Neben den direkt durch das Feuer verursachten Schäden müssen auch die Folgeschäden betrachtet werden.

So dauert die Wiederinbetriebnahme durch Brand beschädigter Bereiche in der Regel Wochen oder gar Monate. Eine sehr große Gefahr bei einem Feuer ist der giftige Brandrauch. Die meisten Personenschäden entstehen daher durch Rauchvergiftungen. Aber auch an Einrichtungen und IT-Systemen kann Brandrauch schwere Schäden anrichten.

Wenn PVC verbrennt, entstehen etwa Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise auch Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen.

## 2.2. Blitz

Während eines Gewitters sind Blitzeinschläge die größte Gefahr für Gebäude und Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50 bis 100 Mikrosekunden freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von etwa zwei Kilometern einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen zu, je näher am Gebäude der Blitz einschlägt.

Schlägt der Blitz direkt in ein Gebäude ein, können durch die dynamische Energie des Blitzes große Schäden verursacht werden. Dies können zum Beispiel Beschädigungen an Dach und Fassade sowie Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.

## 2.3. Wasser

Wasser kann von außen, beispielsweise durch Regen, Hochwasser oder Überschwemmungen, oder von innen, etwa durch defekte wasserführende Leitungen, Schäden an einem Gebäude und seinen Einrichtungen verursachen.

## 2.4. Elementarschäden und Naturkatastrophen

Je nach Standort ist ein Gebäude den Risiken durch Elementarschäden und Naturkatastrophen unterschiedlich stark ausgesetzt. Ursachen für Naturkatastrophen können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen oder Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Starkregen.

## 2.5. Umfeld-Gefährdungen

Gebäude können auch durch Ereignisse in der unmittelbaren Umgebung beschädigt werden, beispielsweise wenn giftige Substanzen austreten. Durch Rettungsarbeiten, Straßensperrungen oder Evakuierungen kann es auch möglich sein, dass das Gebäude nur noch eingeschränkt oder nicht mehr genutzt werden kann.

## 2.6. Unbefugter Zutritt

Wenn Unbefugte in ein Gebäude oder einzelne Räume gelangen, kann dies verschiedene andere Gefährdungen nach sich ziehen. Unbefugte Personen können einerseits durch vorsätzliche Handlungen wie Diebstahl oder Manipulation von Informationen, IT-Systemen oder IT-Komponenten, andererseits aber auch durch unbeabsichtigtes Fehlverhalten, z. B. aufgrund mangelnder Fachkenntnisse, Schäden verursachen.

Dabei können nicht offensichtliche Manipulationen weit höhere Schäden verursachen als direkte Zerstörung. Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt. Diese zu reparieren oder zu ersetzen, beansprucht in der Regel Zeit und finanzielle Mittel, in der diese ihre Schutzfunktion nicht oder nur eingeschränkt bereitstellen.

## 2.7. Verstoß gegen Gesetze oder Regelungen

Wird ein Gebäude errichtet, sind viele Gesetze und Vorgaben zu beachten, die beispielsweise den Brandschutz oder andere Aspekte der baulichen Sicherheit betreffen. Wenn gegen diese Gesetze verstoßen wird, fällt dies unter Umständen lange nicht auf, kann aber katastrophale Folgen nach sich ziehen, etwa wenn Brandschotten nicht bestimmungsgemäß eingebaut wurden.

## 2.8. Unzureichende Brandschottungen

Jedes Gebäude, in dem IT betrieben wird, ist von einer Vielzahl von Kabeln und Leitungen durchzogen, wie beispielsweise Frisch- und Abwasserleitungen, Heizungsrohre oder Leitungen zur Energieversorgung oder Datenübertragung. Es ist dabei unvermeidlich, dass solche Rohr- und Kabeltrassen Brandschutzwände und Geschossdecken queren müssen. Wenn an solchen Stellen keine geeigneten Brandschotten eingebaut sind, können sich darüber unter Umständen Brände und Rauch unkontrolliert ausbreiten.

Die hohe Dynamik der IT macht es auch im Leitungsnetz immer wieder erforderlich, dass Kabel auch über Brandschotten hinweg nachverlegt werden müssen. In welcher Form dies korrekt erfolgen kann, ist unmittelbar von dem vorhandenen Schott abhängig und kann sehr unterschiedlich sein. Werden Änderungen an einem Brandschott nicht nach den Vorgaben des jeweiligen Unternehmens, das das Schott herstellt, ausgeführt, kann es im Fall eines Brandes versagen. Der Brand könnte sich dann in Bereiche ausweiten, die eigentlich durch das Schott geschützt wären.

## 2.9. Ausfall der Stromversorgung

Bei einem Stromausfall können ganze Gebäude oder Teile davon unbenutzbar werden. Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher wie IT oder Beleuchtung abhängig. Auch alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen, Sprinkler- oder Telefonnebenstellenanlagen. Selbst die Wasserversorgung ist in Hoch- oder Tiefgeschossen aufgrund der erforderlichen Pumpen auf Strom angewiesen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.1 *Allgemeines Gebäude* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Haustechnik
Weitere Zuständigkeiten	Mitarbeitende, Planende, Errichterfirma, Zentrale Verwaltung, Bauleitung, Haustechnik, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singularen oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### INF.1.A1 Planung der Gebäudeabsicherung (B) [Planende]

Je nach der (geplanten) Nutzung eines Gebäudes und dem Schutzbedarf der dort betriebenen Geschäftsprozesse MUSS festgelegt werden, wie das Gebäude abzusichern ist. Bei einem Gebäude MÜSSEN insbesondere Sicherheitsaspekte zum Schutz von Personen im Gebäude, dem Schutz der Wirtschaftsgüter und der IT beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Die Sicherheitsanforderungen aus den verschiedenen Bereichen MÜSSEN aufeinander abgestimmt werden.

**INF.1.A2 Angepasste Aufteilung der Stromkreise (B)**

Es MUSS regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen.

**INF.1.A3 Einhaltung von Brandschutzvorschriften (B)**

Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht MÜSSEN eingehalten werden. Die Fluchtwege MÜSSEN vorschriftsmäßig ausgeschildert und freigehalten werden. Es MUSS regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Gebäude in einer Gefahrensituation schnell geräumt werden kann. Bei der Brandschutzplanung SOLLTE die örtliche Feuerwehr hinzugezogen werden.

Unnötige Brandlasten MÜSSEN vermieden werden.

Es MUSS eine Brandschutzbeauftragte oder einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person geben. Diese Person MUSS geeignet geschult sein.

**INF.1.A4 Branderkennung in Gebäuden (B) [Planende]**

Gebäude MÜSSEN entsprechend der Auflagen in der Baugenehmigung und dem Brandschutzkonzept folgend mit einer ausreichenden Anzahl von Rauchmeldern ausgestattet sein. Ist eine lokale Alarmierung am Ort des Melders nicht ausreichend, MÜSSEN alle Melder auf eine Brandmeldezentrale (BMZ) aufgeschaltet werden. Bei Rauchdetektion MUSS eine Alarmierung im Gebäude ausgelöst werden. Es MUSS sichergestellt sein, dass alle im Gebäude anwesenden Personen diese wahrnehmen können. Die Funktionsfähigkeit aller Rauchmelder sowie aller sonstigen Komponenten einer Brandmeldeanlage (BMA) MUSS regelmäßig überprüft werden.

**INF.1.A5 Handfeuerlöscher (B)**

Zur Sofortbekämpfung von Bränden MÜSSEN Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Die Handfeuerlöscher MÜSSEN regelmäßig geprüft und gewartet werden. Die Mitarbeitenden SOLLTEN in die Benutzung der Handfeuerlöscher eingewiesen werden. Die Einweisungen SOLLTEN in zweckmäßigen Zeitabständen wiederholt werden.

**INF.1.A6 Geschlossene Fenster und Türen (B) [Mitarbeitende]**

Fenster und von außen zugängliche Türen, etwa von Balkonen oder Terrassen, MÜSSEN zu Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Räume MÜSSEN verschlossen werden, falls dort vertrauliche Informationen zurückgelassen werden. Dafür MUSS es eine entsprechende Anweisung geben. Alle Mitarbeitenden SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Es MUSS regelmäßig überprüft werden, ob die Fenster und Innen- sowie Außentüren nach Verlassen des Gebäudes verschlossen sind. Brand- und Rauchschutztüren DÜRFEN NUR dann dauerhaft offen gehalten werden, wenn dies durch zugelassene Feststellanlagen erfolgt.

**INF.1.A7 Zutrittsregelung und -kontrolle (B) [Zentrale Verwaltung]**

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen MUSS geregelt und kontrolliert werden. Es SOLLTE ein Konzept für die Zutrittskontrolle existieren. Die Zahl der zutrittsberechtigten Personen SOLLTE für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen DÜRFEN erst Zutritt erhalten, nachdem geprüft wurde, ob dies notwendig ist. Alle erteilten Zutrittsberechtigungen SOLLTEN dokumentiert werden. Die Zutrittskontrollmaßnahmen MÜSSEN regelmäßig auf ihre Wirksamkeit überprüft werden.

Zutrittskontrollen SOLLTEN auch während Umzügen soweit wie möglich vorhanden sein.

**INF.1.A8 Rauchverbot (B)**

Für Räume mit IT oder Datenträgern, in denen Brände oder Verschmutzungen zu hohen Schäden führen können, wie Serverräume, Datenträger- oder Belegarchive, MUSS ein Rauchverbot erlassen werden. Es MUSS regelmäßig kontrolliert werden, dass bei der Einrichtung oder Duldung von Raucherzonen der Zutrittschutz nicht umgangen wird.

**INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften (B) [Errichterfirma, Bauleitung]**

Bei der Planung, der Errichtung und dem Umbau von Gebäuden sowie beim Einbau von technischen Einrichtungen MÜSSEN alle relevanten Normen und Vorschriften berücksichtigt werden.

**3.2. Standard-Anforderungen**

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

**INF.1.A9 Sicherheitskonzept für die Gebäudenutzung (S) [Planende]**

Es SOLLTE ein Sicherheitskonzept für die Gebäudenutzung geben. Das Sicherheitskonzept für das Gebäude SOLLTE mit dem Gesamtsicherheitskonzept der Institution abgestimmt sein. Es SOLLTE dokumentiert und regelmäßig aktualisiert werden.

Schützenswerte Räume oder Gebäudeteile SOLLTEN nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein.

Es MUSS ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden.

**INF.1.A11 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**INF.1.A12 Schlüsselverwaltung (S)**

Für alle Schlüssel des Gebäudes SOLLTE ein Schließplan vorliegen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln SOLLTE zentral geregelt sein. Reserveschlüssel SOLLTEN vorgehalten und gesichert, aber für Notfälle griffbereit aufbewahrt werden. Nicht ausgegebene Schlüssel SOLLTEN sicher aufbewahrt werden. Jede Schlüsselausgabe SOLLTE dokumentiert werden.

**INF.1.A13 Regelungen für Zutritt zu Verteilern (S)**

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen in einem Gebäude SOLLTE im Bedarfsfall schnell möglich sein. Der Zutritt zu Verteilern SOLLTE auf einen engen Kreis von Berechtigten beschränkt sein

**INF.1.A14 Blitzschutzeinrichtungen (S)**

Es SOLLTE eine Blitzschutzanlage nach geltender Norm installiert sein. Es SOLLTE ein umfassendes Blitz- und Überspannungsschutzkonzept vorhanden sein. Die Fangeinrichtungen bei Gebäuden mit umfangreicher IT-Ausstattung SOLLTEN mindestens der Schutzklasse II gemäß DIN EN 62305 Blitzschutz entsprechen. Die Blitzschutzanlage SOLLTE regelmäßig geprüft und gewartet werden.

**INF.1.A15 Lagepläne der Versorgungsleitungen (S)**

Es SOLLTEN aktuelle Lagepläne aller Versorgungsleitungen existieren. Es SOLLTE geregelt sein, wer die Lagepläne aller Versorgungsleitungen führt und aktualisiert. Die Pläne SOLLTEN so aufbewahrt werden, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber im Bedarfsfall schnell verfügbar sind.

**INF.1.A16 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile (S)**

Lagehinweise auf schutzwürdige Bereiche SOLLTEN vermieden werden. Schutzwürdige Gebäudebereiche SOLLTEN von außen nicht leicht einsehbar sein.

**INF.1.A17 Baulicher Rauchschutz (S) [Planende]**

Der bauliche Rauchschutz SOLLTE nach Installations- und Umbauarbeiten überprüft werden. Es SOLLTE regelmäßig überprüft werden, ob die Rauchschutz-Komponenten noch funktionieren.

**INF.1.A18 Brandschutzbegehungen (S)**

Brandschutzbegehungen SOLLTEN regelmäßig, d. h. mindestens ein- bis zweimal im Jahr, stattfinden. Bei Brand-schutzbegehungen festgestellte Mängel SOLLTEN unverzüglich behoben werden.

**INF.1.A19 Information des oder der Brandschutzbeauftragten (S)**

Der oder die Brandschutzbeauftragte SOLLTE über Arbeiten an Leitungstrassen, Fluren, Flucht- und Rettungswegen informiert werden. Diese Person SOLLTE die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren.

**INF.1.A20 Alarmierungsplan und Brandschutzübungen (S)**

Es SOLLTE ein Alarmierungsplan für die im Brandfall zu ergreifenden Maßnahmen erstellt werden. Der Alarmierungsplan SOLLTE in regelmäßigen Abständen überprüft und aktualisiert werden. Brandschutzübungen SOLLTEN regelmäßig durchgeführt werden.

**INF.1.A27 Einbruchschutz (S)**

Es SOLLTEN ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchschutz umgesetzt werden. Bei der Planung, der Umsetzung und im Betrieb SOLLTE beim Einbruchschutz darauf geachtet werden, dass er gleichwertig und durchgängig ist. Er SOLLTE regelmäßig durch eine fachkundige Person begutachtet werden. Die Regelungen zum Einbruchschutz SOLLTEN den Mitarbeitenden bekannt sein.

**INF.1.A36 Regelmäßige Aktualisierungen der Dokumentation (S)**

Die Dokumentation eines Gebäudes, z. B. Baupläne, Trassenpläne, Strangschemata, Fluchtwegpläne und Feuerwehrlaufkarten, SOLLTE immer auf dem aktuellen Stand gehalten werden. Es SOLLTE mindestens einmal innerhalb von drei Jahren überprüft werden, ob alle relevanten Pläne noch aktuell und korrekt sind. Über Änderungen SOLLTEN die Mitarbeitenden informiert werden.

### 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

**INF.1.A21 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

**INF.1.A22 Sichere Türen und Fenster (H)**

Türen und Fenster SOLLTEN anhand der Schutzziele des zu sichernden Bereichs und des Schutzbedarfs der Institution in der passenden Klassifizierung nach den einschlägigen Normen ausgewählt werden. Alle raumumschließenden Sicherungsmaßnahmen durch Fenster, Türen und Wände SOLLTEN in Bezug auf Einbruch, Brand und Rauch gleichwertig und angemessen sein. Es SOLLTE regelmäßig überprüft werden, dass die Sicherheitstüren und -fenster funktionstüchtig sind.

**INF.1.A23 Bildung von Sicherheitszonen (H) [Planende]**

Räume ähnlichen Schutzbedarfs SOLLTEN in Zonen zusammengefasst werden, um vergleichbare Risiken einheitlich behandeln und Kosten für erforderliche Sicherungsmaßnahmen reduzieren zu können.

**INF.1.A24 Selbsttätige Entwässerung (H)**

Alle von Wasser gefährdeten Bereiche SOLLTEN mit einer selbsttätigen Entwässerung ausgestattet sein. Es SOLLTE regelmäßig geprüft werden, ob die aktiven und passiven Entwässerungseinrichtungen noch funktionieren.

**INF.1.A25 Geeignete Standortauswahl (H) [Institutionsleitung]**

Bei Planung und Auswahl des Gebäudestandortes SOLLTE geprüft werden, welche Umfeldbedingungen Einfluss auf die Informationssicherheit haben könnten. Es SOLLTE eine Übersicht über standortbedingte Gefährdungen geben. Diesen Gefährdungen SOLLTE mit zusätzlichen kompensierenden Maßnahmen entgegengewirkt werden.

**INF.1.A26 Pforten- oder Sicherheitsdienst (H)**

Die Aufgaben des Pforten- oder Sicherheitsdienstes SOLLTEN klar dokumentiert sein. Der Pfortendienst SOLLTE alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten und, je nach Sicherheitskonzept, kontrollieren. Alle Mitarbeitenden und Besuchenden SOLLTEN sich bei dem Pfortendienst ausweisen können. Besuchende SOLLTEN zu den Besuchten begleitet oder an der Pforte abgeholt werden. Der Pfortendienst SOLLTE rechtzeitig darüber informiert werden, wenn sich Zutrittsberechtigungen ändern.

**INF.1.A28 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

**INF.1.A29 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

**INF.1.A30 Auswahl eines geeigneten Gebäudes (H)**

Bei der Auswahl eines geeigneten Gebäudes SOLLTE geprüft werden, ob alle für die spätere Nutzung relevanten Sicherheitsanforderungen umgesetzt werden können. Für jedes Gebäude SOLLTEN im Vorfeld die vorhandenen Gefährdungen und die erforderlichen Schäden vorbeugenden oder reduzierenden Maßnahmen dokumentiert werden.

**INF.1.A31 Auszug aus Gebäuden (H) [Zentrale Verwaltung]**

Im Vorfeld des Auszugs SOLLTE ein Bestandsverzeichnis aller für die Informationssicherheit für den Umzug relevanten Objekte wie Hardware, Software, Datenträger, Ordner oder Schriftstücke erstellt werden. Nach dem Auszug SOLLTEN alle Räume nach zurückgelassenen Dingen durchsucht werden.

**INF.1.A32 Brandschott-Kataster (H)**

Es SOLLTE ein Brandschott-Kataster geführt werden. In diesem SOLLTEN alle Arten von Schotten individuell aufgenommen werden. Nach Arbeiten an Brandschotten SOLLTEN die Änderungen im Kataster spätestens nach vier Wochen eingetragen werden.

**INF.1.A33 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

**INF.1.A34 Gefahrenmeldeanlage (H)**

Es SOLLTE eine den Räumlichkeiten und den Risiken angemessene Gefahrenmeldeanlage geben. Die Gefahrenmeldeanlage SOLLTE regelmäßig geprüft und gewartet werden. Es MUSS sichergestellt werden, dass diejenigen, die Gefahrenmeldungen empfangen in der Lage sind, technisch und personell angemessen auf den Alarm zu reagieren.

**INF.1.A35 Perimeterschutz (H) [Planende, Haustechnik]**

Abhängig vom Schutzbedarf des Gebäudes und abhängig vom Gelände SOLLTE dieses über einen Perimeterschutz verfügen. Hierbei SOLLTEN mindestens folgende Komponenten auf ihren Nutzen und ihre Umsetzbarkeit hin betrachtet werden:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Maßnahmen zur Erschwerung des beabsichtigten gewaltsamen Überwindens der Grundstücksgrenze,
- Freigelände-Sicherungsmaßnahmen,
- Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (beispielsweise Videoaufzeichnung) sowie
- automatische Alarmierung.

## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF19 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-53 zu „Assessing Security and Privacy Controls for Federal Information Systems and Organizations“ veröffentlicht und macht im Appendix C (Table C-11) Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.



## INF.2 Rechenzentrum sowie Serverraum

### 1. Beschreibung

#### 1.1. Einleitung

Heute werden fast alle strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind ohne IT nicht ausführbar. Dadurch steigen die Anforderungen an die Leistungsfähigkeit und Verfügbarkeit der IT-Systeme und deren Anbindung an die Netzumgebung stetig. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, konzentrieren Institutionen jeglicher Größe ihre IT-Landschaft in Rechenzentren.

Ein Rechenzentrum (RZ) ist wie folgt definiert:

1. Hat eine IT-nutzende Institution nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ entsprechend dem Schutzbedarf zu behandeln. Unter „IT-Betriebsbereich“ sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (z. B. Stromversorgung, Kälteversorgung, Löschanlagen, Sicherheitstechnik), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen.
2. Wird die IT der Institution innerhalb eines Gebäudes oder einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Benutzenden hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als RZ zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr IT-Benutzenden abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als RZ zu behandeln.
3. Ist die IT-nutzende Institution an mehreren räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend (1) separat zu betrachten und zu behandeln.
4. Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben einer Institution führen) erforderliche IT angesiedelt ist, ist immer als RZ zu behandeln, unabhängig von Größe oder Anteilsregeln aus Nummer (2).
5. IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als Teil eines RZ zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.
6. Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt den sich daraus ergebenden Reduzierungen von Sicherheitsanforderungen zu begründen.

Die Auflistung der sechs Punkte bedeutet nicht, dass alle Punkte gemeinsam erfüllt sein müssen, damit ein Bereich als Rechenzentrum betrachtet wird. Vielmehr werden verschiedene Möglichkeiten beschrieben, wann ein Bereich als RZ anzusehen ist. Weicht ein Rechenzentrum von dieser Definition ab, wird der betrachtete IT-Betriebsbereich als Serverraum bezeichnet. Diese Definition orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der nutzenden Institution und steht damit im methodischen Einklang mit der DIN EN 50600.

Soll ein Serverraum abgesichert werden, können die Anforderungen dieses Bausteins entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden (6) und es müssen mindestens die Basis-Anforderungen umgesetzt werden.

## 1.2. Zielsetzung

Dieser Baustein richtet sich einerseits an Institutionen, die ein Rechenzentrum betreiben und im Rahmen einer Revision prüfen möchten, ob sie geeignete Sicherheitsmaßnahmen umgesetzt haben. Andererseits kann der Baustein auch dazu benutzt werden, die Sicherheitsmaßnahmen abzuschätzen, die umgesetzt werden müssen, wenn die IT in einem Rechenzentrum zentralisiert werden soll. Das oberste Ziel der in diesem Baustein beschriebenen Anforderungen ist es, den sicheren Betrieb des Rechenzentrums zu gewährleisten.

## 1.3. Abgrenzung und Modellierung

Der Baustein INF.2 *Rechenzentrum sowie Serverraum* ist auf jedes Rechenzentrum und jeden Serverraum anzuwenden.

Der vorliegende Baustein eignet sich nicht für kleine Informationsverbünde mit z. B. nur einem oder sehr wenigen Servern oder IT-Systemen. Ein Beispiel dafür ist eine kleine Institution mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum betrieben wird. In solchen Fällen genügt es oft, den Baustein INF.5 *Raum sowie Schrank für technische Infrastruktur* umzusetzen.

Anforderungen an Gebäude und die Verkabelung im Allgemeinen sind nicht Teil dieses Bausteins. Diese sind in den Bausteinen INF.1 *Allgemeines Gebäude* und INF.12 *Verkabelung* zu finden, die immer auf Räume und Gebäude bzw. die Verkabelung anzuwenden sind.

Um den Baustein überschaubar zu halten, wurde bewusst auf technische Details und planerische Größen verzichtet. Nähere Informationen liefern einschlägige Normen und weitere Veröffentlichungen des BSI.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.2 *Rechenzentrum sowie Serverraum* von besonderer Bedeutung.

### 2.1. Fehlerhafte Planung

Wenn ein Rechenzentrum konzipiert und dabei nicht berücksichtigt wird, es gegen elementare Gefährdungen abzusichern, besteht ein sehr hohes Ausfallrisiko. So können z. B. Standortrisiken wie Luftverkehr, Erdbeben oder Hochwasser die Betriebssicherheit und Verfügbarkeit gefährden. Ebenso massiv kann es sich auf den Betrieb eines Rechenzentrums auswirken, wenn durch eine fehlerhafte Konzeptionierung nicht genügend Bandbreite verfügbar ist oder die Energieversorgung am gewählten Standort nicht ausreicht.

### 2.2. Fehlende oder fehlerhafte Zutrittskontrollen

Fehlen Zutrittskontrollen oder sind diese unzureichend, erhöht sich die Gefahr, dass unberechtigte Personen das Rechenzentrum betreten und dort fahrlässig, z. B. aufgrund mangelnder Fachkenntnisse, oder vorsätzlich Schaden anrichten. Angreifende können so z. B. schützenswerte Daten entwenden, Geräte stehlen oder Server manipulieren. Unzureichende Zutrittskontrollen wirken sich somit auf die Verfügbarkeit, Vertraulichkeit und die Integrität von Daten und IT-Komponenten aus.

### 2.3. Unzureichende Überwachung

Wird die im Rechenzentrum betriebene IT und Infrastruktur unzureichend überwacht und betreut, können Komponenten unbemerkt ausfallen. Dadurch wird eventuell die Verfügbarkeit und fehlerfreie Funktion des Rechenzentrums stark beeinträchtigt. Ausfälle treten zudem oftmals schlechend ein. Ohne eine aktive Überwachung könnten diese zu spät bemerkt werden. Es ist dann oft nicht mehr möglich, rechtzeitig zu reagieren.

### 2.4. Unzureichende Klimatisierung im Rechenzentrum

IT-Komponenten benötigen bestimmte Betriebsbedingungen, um zuverlässig zu funktionieren. Auch setzen sie die von ihnen aufgenommene elektrische Leistung in zusätzliche Wärme um. Wenn in einem IT-Betriebsbereich die Temperatur, die Luftfeuchte oder der Schwebestoffanteil nicht innerhalb der von den Geräteherstellenden vorgege-

benen Grenzwerte gehalten werden, kann dies dazu führen, dass technische Komponenten nicht mehr richtig funktionieren oder ausfallen.

## 2.5. Feuer

Feuer ist zwar eine Gefahr, die eher selten eintritt. Entsteht aber tatsächlich ein Brand, hat dieser meist schwerwiegende Auswirkungen. Denn durch Feuer und Rauch können große Schäden entstehen. Während innerhalb des IT-Betriebsbereichs Elektrobrände die häufigste Ursache für Feuer sind, kann ein Feuer außerhalb des IT-Betriebsbereichs und insbesondere in Supportbereichen, wie der Energieversorgung (inklusive NEA und USV) oder der Klimaanlage, zahlreiche weitere Ursachen haben. Haben der IT-Betriebsbereich oder die Supportbereiche sowie andere Nachbarbereiche keinen oder nur einen unzureichenden Brandschutz, kann sich ein Feuer schnell ausbreiten. Zudem könnten außerhalb entstehende Brände auf das Rechenzentrum übergreifen.

## 2.6. Wasser

Durch undichte Wasserleitungen, Hochwasser, Rohrbruch, defekte Sprinkler- oder Klimaanlagen kann Wasser in das Rechenzentrum eintreten. Hierdurch können Geräte beschädigt werden und nicht mehr funktionieren. Es kann auch ein Kurzschluss ausgelöst werden, durch den einzelne Bereiche des Rechenzentrums ausfallen oder ein Brand entstehen könnte.

## 2.7. Fehlender oder unzureichender Einbruchsschutz

Selbst wenn eine gut funktionierende Zutrittskontrolle eingerichtet ist, können unbefugte Personen in ein Rechenzentrum eindringen, sofern es nicht ausreichend vor Einbrüchen geschützt wird. Täter und Täterinnen könnten so z. B. IT-Komponenten stehlen oder manipulieren und an vertrauliche Informationen gelangen. Auch könnten sie die Geräte zerstören oder das Rechenzentrum insgesamt beschädigen.

## 2.8. Ausfall der Stromversorgung

Wenn der Strom ausfällt, kann der Betriebsablauf eines Rechenzentrums und damit der Institution erheblich gestört werden. So sind bei einem Stromaussfall eventuell die vom Rechenzentrum bereitgestellten IT-Services plötzlich nicht mehr erreichbar. Ebenso können Daten verloren gehen. Zudem ist es möglich, dass durch einen plötzlichen Stromaussfall IT-Systeme, TK-Systeme oder Überwachungstechnik beschädigt werden.

## 2.9. Verschmutzung

Staub und andere Verschmutzungen in einem Rechenzentrum können dazu führen, dass technische Komponenten (z. B. Lüfter) nicht mehr funktionieren. Durch Verschmutzungen verschleißt Geräte früher und fallen häufiger aus.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.2 *Rechenzentrum sowie Serverraum* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Mitarbeitende, Planende, Datenschutzbeauftragte, Haustechnik, Wartungspersonal

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singularen oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### INF.2.A1 Festlegung von Anforderungen (B) [Haustechnik, Planende]

Für ein Rechenzentrum MÜSSEN angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden.

Wenn ein Rechenzentrum geplant wird oder geeignete Räumlichkeiten ausgewählt werden, MÜSSEN auch geeignete Sicherheitsmaßnahmen unter Berücksichtigung des Schutzbedarfs der IT-Komponenten (insbesondere der Verfügbarkeit) mit geplant werden.

Ein Rechenzentrum MUSS insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Es MUSS zudem unterschiedliche Sicherheitszonen aufweisen. Dafür MÜSSEN z. B. Verwaltungs-, Logistik-, IT-Betriebs- und Support-Bereiche klar voneinander getrennt werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob unterschiedliche Sicherheitszonen eingerichtet werden können.

#### INF.2.A2 Bildung von Brandabschnitten (B) [Planende]

Es MÜSSEN geeignete Brand- und Rauchabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Die Brand- und Rauchabschnitte MÜSSEN über den baurechtlich vorgeschriebenen Rahmen hinaus auch Schutz für die darin befindlichen technischen Einrichtungen und deren Verfügbarkeit bieten. Es MUSS verhindert werden, dass sich Brand und Rauch ausbreiten. Im Falle eines Serverraums SOLLTE geprüft werden, ob geeignete Brand- und Rauchabschnitte für die Räumlichkeiten umsetzbar sind.

#### INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung (B) [Haustechnik]

Für alle betriebsrelevanten Komponenten des Rechenzentrums MUSS eine unterbrechungsfreie Stromversorgung (USV) installiert werden. Da der Leistungsbedarf von Klimaanlagen oft zu hoch für eine USV ist, MUSS mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen werden. Im Falle eines Serverraums SOLLTE je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist.

Die USV MUSS ausreichend dimensioniert sein. Bei relevanten Änderungen an den Verbrauchern MUSS überprüft werden, ob die vorhandenen USV-Systeme noch ausreichend dimensioniert sind.

Bei USV-Systemen mit Batterie als Energiespeicher MUSS die Batterie im erforderlichen Temperaturbereich gehalten werden. Sie SOLLTE dazu vorzugsweise räumlich getrennt von der Leistungselektronik der USV platziert werden. Die USV MUSS regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür MÜSSEN die vom herstellenden Unternehmen vorgesehenen Wartungsintervalle eingehalten werden.

#### INF.2.A4 Notabschaltung der Stromversorgung (B) [Haustechnik]

Es MUSS geeignete Möglichkeiten geben, elektrische Verbraucher im Rechenzentrum spannungsfrei zu schalten. Dabei MUSS darauf geachtet werden, ob und wie eine vorhandene USV räumlich und funktional in die Stromversorgung eingebunden ist. Werden klassische Not-Aus-Schalter eingesetzt, MUSS darauf geachtet werden, dass darüber nicht das komplette Rechenzentrum abgeschaltet wird. Die Notabschaltung MUSS sinnvoll parzelliert und zielgerichtet erfolgen. Alle Not-Aus-Schalter MÜSSEN so geschützt sein, dass sie nicht unbeabsichtigt oder unbefugt betätigt werden können.

#### INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit (B) [Haustechnik]

Es MUSS sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzwerte liegen. Die tatsächliche Wärmelast in den gekühlten Bereichen MUSS in regelmäßigen Abständen und nach größeren Umbauten überprüft werden.

Eine vorhandene Klimatisierung MUSS regelmäßig gewartet werden. Die Parameter Temperatur und Feuchtigkeit MÜSSEN mindestens so aufgezeichnet werden, dass sich rückwirkend erkennen lässt, ob Grenzwerte überschritten wurden, und dass sie bei der Lokalisierung der Ursache der Abweichung sowie bei der Beseitigung der Ursache unterstützend genutzt werden können.

## INF.2.A6 Zutrittskontrolle (B) [Haustechnik]

Der Zutritt zum Rechenzentrum MUSS kontrolliert werden. Zutrittsrechte MÜSSEN gemäß der Vorgaben des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* vergeben werden. Für im Rechenzentrum tätige Personen MUSS sichergestellt werden, dass diese keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.

Alle Zutrittsmöglichkeiten zum Rechenzentrum MÜSSEN mit Zutrittskontrolleinrichtungen ausgestattet sein. Jeder Zutritt zum Rechenzentrum MUSS von der Zutrittskontrolle individuell erfasst werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.

Es MUSS regelmäßig kontrolliert werden, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden.

Die Anforderungen der Institution an ein Zutrittskontrollsyste MÜSSEN in einem Konzept ausreichend detailliert dokumentiert werden.

## INF.2.A7 Verschließen und Sichern (B) [Mitarbeitende, Haustechnik]

Alle Türen des Rechenzentrums MÜSSEN stets verschlossen gehalten werden. Fenster MÜSSEN möglichst schon bei der Planung vermieden werden. Falls sie doch vorhanden sind, MÜSSEN sie ebenso wie die Türen stets verschlossen gehalten werden. Türen und Fenster MÜSSEN einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffe und Umgebungseinflüsse bieten. Sie MÜSSEN mit einem Sichtschutz versehen sein. Dabei MUSS beachtet werden, dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die erforderliche Schutzwirkung gleichwertig sein muss.

## INF.2.A8 Einsatz einer Brandmeldeanlage (B) [Planende]

In einem Rechenzentrum MUSS eine Brandmeldeanlage installiert sein. Diese MUSS alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage MÜSSEN geeignet weitergeleitet werden (siehe dazu auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen*). Die Brandmeldeanlage MUSS regelmäßig gewartet werden. Es MUSS sichergestellt werden, dass in Räumen des Rechenzentrums keine besonderen Brandlasten vorhanden sind.

## INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage (B) [Haustechnik]

In einem Rechenzentrum MUSS entweder eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein oder durch technische (insbesondere durch eine flächendeckende Brandfrüherkennung, siehe INF.2.A17 *Brandfrüherkennung*) und organisatorische Maßnahmen (geschultes Personal und Reaktionspläne für Meldungen der Brandfrüherkennung) sichergestellt sein, dass unmittelbar (innerhalb von maximal 3 Minuten) auf Meldungen der Brandfrüherkennung mit schadensminimierenden Maßnahmen reagiert wird.

In Serverräumen ohne Lösch- oder Brandvermeidungsanlage MÜSSEN Handfeuerlöscher mit geeigneten Löschmitteln in ausreichender Zahl und Größe vorhanden sein. Es MUSS beachtet werden, dass darüber hinausgehende baurechtliche Anforderungen hinsichtlich der Ausstattung mit Handfeuerlöschern davon unberührt bleiben. Die Feuerlöscher MÜSSEN so angebracht werden, dass sie im Brandfall leicht zu erreichen sind. Jeder Feuerlöscher MUSS regelmäßig geprüft und gewartet werden. Alle Mitarbeitenden, die ein Rechenzentrum oder einen Serverraum betreten dürfen, MÜSSEN in die Benutzung der Handfeuerlöscher eingewiesen werden.

## INF.2.A10 Inspektion und Wartung der Infrastruktur (B) [Wartungspersonal, Haustechnik]

Für alle Komponenten der baulich-technischen Infrastruktur MÜSSEN mindestens die vom herstellenden Unternehmen empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Inspektionen und Wartungsarbeiten MÜSSEN protokolliert werden. Brandschotten MÜSSEN daraufhin geprüft werden, ob sie unversehrt sind. Die Ergebnisse MÜSSEN dokumentiert werden.

## INF.2.A11 Automatische Überwachung der Infrastruktur (B) [Haustechnik]

Alle Einrichtungen der Infrastruktur, wie z. B. Leckageüberwachung, Klima-, Strom- und USV-Anlagen, MÜSSEN automatisch überwacht werden. Erkannte Störungen MÜSSEN schnellstmöglich in geeigneter Weise weitergeleitet und bearbeitet werden.

Im Falle eines Serverraums SOLLTEN IT- und Supportgeräte, die nicht oder nur selten von einer Person bedient werden müssen, mit einer Fernanzeige für Störungen ausgestattet werden. Die verantwortlichen Mitarbeitenden MÜSSEN zeitnah alarmiert werden.

**INF.2.A17 Einsatz einer Brandfrüherkennung (B) [Planende, Haustechnik]**

Ein Rechenzentrum MUSS mit einer Brandfrüherkennungsanlage ausgestattet werden. Ein Serverraum SOLLTE mit einer Brandfrüherkennungsanlage ausgestattet werden. Die Meldungen der Brandfrüherkennung MÜSSEN an eine ständig besetzte Stelle geleitet werden, die eine Kontrolle und Schutzreaktion innerhalb von maximal 3 Minuten veranlassen kann. Alternativ MUSS eine automatische Schutzreaktion erfolgen. Um ein ausgewogenes Verhältnis zwischen Brandschutz und Verfügbarkeit zu erreichen, MUSS sichergestellt werden, dass sich einander Redundanz gebende Einrichtungen nicht gemeinsam im Wirkungsbereich der gleichen Spannungsfreischaltung befinden.

**INF.2.A29 Vermeidung und Überwachung nicht erforderlicher Leitungen (B) [Haustechnik, Planende]**

In einem Rechenzentrum DÜRFEN NUR Leitungen verlegt werden, die der unmittelbaren Versorgung der im Rechenzentrum aufgebauten Technik (in der Regel IT- und gegebenenfalls Kühltechnik) dienen. Ist es aus baulichen Gründen unabwendbar, Leitungen durch das Rechenzentrum zu führen, um andere Bereiche als die des Rechenzentrums zu versorgen, MUSS dies einschließlich Begründung dokumentiert werden. Die Risiken, die von solchen Leitungen ausgehen, MÜSSEN durch geeignete Maßnahmen minimiert werden, z. B. durch Einhausung und Überwachung.

Durch Serverräume dürfen vorgenannte Leitungen geführt werden, ohne zu begründen, warum dies unabwendbar ist, diese MÜSSEN aber genauso behandelt werden, wie für das Rechenzentrum beschrieben.

Meldungen aus der Überwachung der Leitungen MÜSSEN unverzüglich hinsichtlich der Gefährdungsrelevanz geprüft und bewertet werden. Gegenmaßnahmen MÜSSEN entsprechend der erkannten Gefährdungsrelevanz zeitgerecht umgesetzt werden (siehe auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen*).

### 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

**INF.2.A12 Perimeterschutz für das Rechenzentrum (S) [Planende, Haustechnik]**

Für Rechenzentren SOLLTE ein Perimeterschutz existieren. Je nach festgelegtem Schutzbedarf für das Rechenzentrum und abhängig vom Gelände SOLLTE der Perimeterschutz aus folgenden Komponenten bestehen:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze,
- Freiland-Sicherungsmaßnahmen,
- äußere Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (beispielsweise Videoaufzeichnung) sowie
- automatische Alarmierung.

**INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen (S) [Haustechnik]**

Basierend auf dem Sicherheitskonzept des Gebäudes SOLLTE geplant werden, welche Gefahrenmeldeanlagen für welche Bereiche des Rechenzentrums benötigt und installiert werden. Hierüber hinaus SOLLTE festgelegt werden, wie mit Alarmmeldungen umzugehen ist. Das Konzept SOLLTE immer angepasst werden, wenn sich die Nutzung der Gebäudebereiche verändert.

Es SOLLTE eine zum jeweiligen Einsatzzweck passende Gefahrenmeldeanlage (GMA) installiert werden. Die Meldungen der GMA SOLLTEN unter Beachtung der dafür geltenden Technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle aufgeschaltet werden. Die ausgewählte Alarmempfangsstelle MUSS jederzeit erreichbar sein. Sie MUSS technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren. Der Übertragungsweg zwischen eingesetzter GMA und Alarmempfangsstelle SOLLTE entsprechend den TAB und nach Möglichkeit redundant ausgelegt werden. Alle vorhandenen Übertragungswege MÜSSEN regelmäßig getestet werden.